Quantum String Seal Is Insecure

H. F. Chau*
Department of Physics, University of Hong Kong, Pokfulam Road, Hong Kong and
Center of Theoretical and Computational Physics,
University of Hong Kong, Pokfulam Road, Hong Kong
(Dated: February 1, 2008)

A quantum string seal encodes the value of a (bit) string as a quantum state in such a way that everyone can extract a non-negligible amount of available information on the string by a suitable measurement. Moreover, such measurement must disturb the quantum state and is likely to be detected by an authorized verifier. In this way, the intactness of the encoded quantum state plays the role of a wax seal in the digital world. Here I analyze the security of quantum string seal by studying the information disturbance tradeoff of a measurement. This information disturbance tradeoff analysis extends the earlier results of Bechmann-Pasquinucci *et al.* and Chau by concluding that all quantum string seals are insecure. Specifically, I find a way to obtain non-trivial available information on the string that escapes the verifier's detection with at least 50% chance.

PACS numbers: 03.67.Dd, 03.67.Hk, 89.20.Ff, 89.70.+c
Keywords: Information disturbance tradeoff, Post-modern quantum cryptography, Quantum seal

I. INTRODUCTION

The idea of quantum seal was introduced by Bechmann-Pasquinucci to capture the essence of an envelop with sealed wax in the digital world [1]. Specifically, a quantum (bit) seal is a method to encode a classical bit by some quantum particles in such a way that everyone can find out the value of the bit with high chance by an appropriate measurement. Moreover, any such measurement must disturb the state of the quantum particles so that an authorized person, who has some extra information on the state of the particles, can detect such a measurement with high probability [1].

A few quantum sealing schemes have been proposed. They fall into the following three types. The original scheme by Bechmann-Pasquinucci [1] and the one by Chau [2] are perfect quantum bit seals because everyone can find out the value of the bit with certainty. The quantum bit seals introduced by Singh and Srikanth [3] as well as He [4] are imperfect quantum bit seals as readers cannot correctly determine the value of the bit with certainty. Recently, He [5] extended the notion of sealing a bit to sealing a bit string in a natural way by proposing an imperfect quantum bit string seal which separately encodes each bit of a classical string. Parameters in He's scheme are set in such a way that one has a high chance to correctly extract a large portion of the string. However, one has negligibly small chance to correctly determine the whole string [5].

Density matrices representing any two distinct classical messages in a perfect quantum seal must be orthogonal. Hence, there exits a projective measurement to find out the encoded message without disturbing the quantum state. Using this idea, Bechmann-Pasquinucci *et al.* proved the insecurity of all perfect quantum (bit) seals provided that one has access to a quantum computer [6]. Recently, He showed certain bounds relating the information gain and the measurement detection probability for any quantum bit seal [7]. However, his bound is not tight. In contrast, Chau proved that all imperfect quantum bit seals are insecure by giving an explicit measurement strategy. In addition, he obtained a lower bound for the fidelity of the resultant quantum state after a measurement. More importantly, this lower bound is greater than 1/2 and is attainable by certain quantum sealing schemes [8].

The insecurity proof by Chau in Ref. [8] relies heavily on the properties of trace distance between two density matrices. Generalizing his proof to the case of sealing more than two classical states is not straight-forward. Furthermore, the security analysis of quantum string commitment by Buhrman *et al.* [9, 10] illustrated two important points. First, more than one inequivalent security parameters may exist for a quantum string cryptographic scheme; and second, the security of a quantum string cryptographic scheme may be very different from that of a quantum bit one. Therefore, it is important to study the security of quantum string seal thoroughly.

In this Paper, I analyze the information disturbance tradeoff for a general quantum seal that maps a fixed number N of distinct classical messages to N density matrices. Moreover, the probabilities of occurrence of these classical messages need not be equal. I begin by introducing the general formalism and the security requirements for a quantum seal as well as the notion of the most stringent quantum seal in Sec. II. Then I report a measurement strategy that obtains non-zero amount of information on the original message and introduce two performance measures in Sec. III. I also prove the optimality of this measurement strategy against the most stringent quantum seal under one of the performance measures. And I also argue that this strategy also performs well

*Electronic address: hfchau@hkusua.hku.hk

under the other performance measure in Sec. III. Using these information disturbance analyses, I show that all imperfect quantum seals, including quantum string seals in which $N = 2^n$, are insecure in Sec. IV. Finally, a summary is given in Sec. V.

II. QUANTUM SEAL

A. Quantum seal and its security requirements

A quantum seal is a scheme for Alice to encode a fixed number N of distinct classical messages as publicly accessible quantum mixed states known as the sealed states. (Although N is a fixed integer and the dimension of the sealed states is finite, readers can check that the proofs and discussions reported in this paper can be easily extended to the case when the number of distinct classical messages N as well as the dimension of the quantum mixed states involved are infinite.) It has to satisfy:

1. Any member of the public, say Bob, can correctly determine a significant portion of the original classical message chosen by Alice, known as the sealed message, with non-negligible probability by a measurement.

2. Any such measurement in criterion 1 must disturb the sealed state so that an authorized verifier may correctly detect the measurement with non-zero (unconditional) probability.

3. Criterion 2 still holds after replacing the unconditional probability by the probability conditioned on Bob's successful determination of a significant portion of the sealed message.

In the language of information theory, criterion 1 means that the mutual information on the sealed message obtained by Bob divided by the entropy of the original classical message is of order of 1. Clearly, this criterion is necessary; for otherwise, even an honest Bob has negligible chance to obtain a significant fraction of the sealed message.

The maximum probability for Bob to correctly determine the sealed message can be made close to $1/N$. Nonetheless, in order to satisfy criterion 1, there exists a partition $\mathfrak{P}$ of the N distinct classical messages with $\log|\mathfrak{P}| \lesssim \log N$ such that the maximum probability of correctly determining which set in the partition the original message belongs to is much greater than $1/|\mathfrak{P}|$. (Let's use He's quantum string scheme as an example to illustrate this point. Although it is not likely to correctly extract the entire sealed string in He's scheme, it is highly probable to correctly determine, say, the first 99% of the sealed string [5]. In fact, one possible choice of $\mathfrak{P}$ in this case is to partition according to the values of the first 99% of the original message string.) Through the partition $\mathfrak{P}$, the quantum seal that encodes N distinct classical messages can be regarded as a seal that encodes $|\mathfrak{P}|$ distinct classical messages. With this identification in mind, I may assume from now on that the maximum probability of correctly finding the original classical message $p_{\max}$ to be much greater than $1/N$. Furthermore, without loss of generality, I label these N classical messages by $0, 1, \ldots, N-1$ in such a way that the *a priori* probability of occurrence η_i for the message i obeys the constraints $\eta_0 \geq \eta_1 \geq \cdots \geq \eta_{N-1} > 0$ and $\sum_{i=0}^{N-1} \eta_i = 1$.

A quantum sealing scheme is called a *quantum bit seal* if $N = 2$ and a *quantum (bit) string seal* if $N = 2^n$. Moreover, the scheme is *perfect* if Bob can determine the entire classical message with certainty; otherwise, the scheme is *imperfect* [8].

B. A game-theoretic formulation of the problem

Quantum seal is in some sense a game between Alice and Bob. For a given sealing scheme used by Alice, Bob tries to gain as much information on the sealed message as possible on the one hand and to reduce the chance of being caught by the verifier on the other hand. And Alice surely wants to pick a sealing scheme that makes Bob's task as difficult as possible.

To analyze the security of quantum seals, all sealed states can be assumed to be pure as using purified states increase the verifier's chance to detect Bob's measurement [8]. Using the notation used in Ref. [8], the sealed state for message i is

$$|\tilde{\psi}_i\rangle = \sum_j \lambda_{ij} |\psi_{ij}\rangle_{\rm B} \otimes |\phi_j\rangle_{\rm A} \tag{1}$$

for all i, where $|\psi_{ij}\rangle$'s are normalized states that are not necessarily mutually orthogonal, and $|\phi_j\rangle$'s are orthonormal states. Note that particles labeled by the subscript "B" in Eq. (1) are publicly accessible, and those labeled by the subscript "A" are accessible only to authorized verifiers. Thus, the state of the publicly accessible particles is

$$\rho_i = \sum_j |\lambda_{ij}|^2 |\psi_{ij}\rangle\langle\psi_{ij}| \ . \tag{2}$$

if the sealed message is i.

Bob's attempt to obtain some information on the classical message can be described by a positive operator-valued measure (POVM) measurement $\mathcal{E}$ on the publicly accessible particles. From the verifier's point of view, this measurement changes the sealed state $|\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|$ to $\mathcal{E} \otimes I(|\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|) \equiv \tilde{\mathcal{E}}(|\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|)$.

I write $\mathcal{E} = \sum_{j=0}^{N-1} \mathcal{L}_j$, where $\mathcal{L}_j$ is the superoperator describing Bob's action when he concludes that the sealed message is j. Then, the probability that Alice's original message is i and Bob's measurement on the sealed state yields j is given by

$$\Pr_{ij} = \eta_i {\rm Tr}[\mathcal{L}_j \otimes I(|\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|)] \equiv \eta_i {\rm Tr}[\tilde{\mathcal{L}}_j(|\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|)] \ . \tag{3}$$

In addition, Bob's mutual information on the original message equals

$$\begin{aligned}\mathcal{I} &\equiv \mathcal{I}(\mathcal{E}) \equiv \mathcal{I}(\tilde{\mathcal{E}}) \\ &= -\sum_i \eta_i \log_2 \eta_i - \sum_j \left(\sum_k \Pr_{kj}\right) \log_2 \left(\sum_k \Pr_{kj}\right) \\ &\quad + \sum_{i,j} \Pr_{ij} \log_2 \Pr_{ij} \ . \end{aligned} \tag{4}$$

A simple way to measure Bob's average chance of being caught is to compute the average fidelity of the sealed state [8], namely,

$$\bar{F} \equiv \bar{F}(\mathcal{E}) \equiv \bar{F}(\tilde{\mathcal{E}}) = \sum_{i=0}^{N-1} \eta_i \langle\tilde{\psi}_i|\tilde{\mathcal{E}}(|\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|)|\tilde{\psi}_i\rangle \ . \tag{5}$$

In other words, the average fidelity (or fidelity for short) $\bar{F}$ measures the mean disturbance caused by Bob's measurement $\mathcal{E}$. Since $1-\bar{F}$ is the probability of detecting Bob's measurement, $\bar{F}$ is a performance indicator for criterion 2 stated in Subsec. II A.

Bob's chance of being caught given that he correctly determined the sealed message is reflected in the average fidelity of the sealed state conditional on Bob's success $\bar{F}_{\rm cond}$, namely,

$$\begin{aligned}\bar{F}_{\rm cond} &\equiv \bar{F}_{\rm cond}(\mathcal{E}) \equiv \bar{F}_{\rm cond}(\tilde{\mathcal{E}}) \\ &= \sum_{i=0}^{N-1} \frac{\eta_i \langle\tilde{\psi}_i|\tilde{\mathcal{L}}_i(|\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|)|\tilde{\psi}_i\rangle}{{\rm Tr}[\tilde{\mathcal{L}}_i(|\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|)]} \ . \end{aligned} \tag{6}$$

(Note that those terms with ${\rm Tr}[\tilde{\mathcal{L}}_i(|\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|)] = 0$ in the above equation are regarded as 0.) Thus, the average conditional fidelity (or conditional fidelity for short) $\bar{F}_{\rm cond}$ measures the mean disturbance caused by Bob's measurement $\mathcal{E}$ conditioned on his successful recovery of the sealed message. Since $1-\bar{F}_{\rm cond}$ is the probability of detecting Bob's measurement conditioned on Bob's successful recovery of the sealed message, $\bar{F}_{\rm cond}$ is a performance indicator for criterion 3 in Subsec. II A.

I denote the probability of correctly determining the sealed message using the POVM measurement $\mathcal{E}$ by p. Surely, $p \le p_{\max}$. Furthermore, I assume $p \ge 1/N$ as no one is interested in those $\mathcal{E}'s$ that perform worse than random guessing. (Interestingly, the scheme with $\eta_i = 1/N$ and $\rho_i = \rho_j$ for all i, j illustrates that p may not be less than $1/N$.)

Amongst all the POVM's whose probability of correctly determining the sealed message is p, Bob would like to pick the one that minimizes the average chance of being detected by a verifier (and hence maximizes $\bar{F}$). In contrast, Alice would like to pick a seal that minimizes $\bar{F}$. Thus, the average fidelity $\min_{\rm Alice}\max_{\rm Bob}\bar{F}(p, p_{\max})$ for the optimal measurement strategy against the most stringent seal is found by first taking the maximum over all possible POVM measurements $\mathcal{E}$'s used by Bob whose probability of correctly determining the original message is p for a given sealing scheme, and then by taking the minimum over all quantum seals with maximum probability of correctly determining the message $p_{\max}$ by Alice [8]. The average conditional fidelity for the optimal measurement strategy against the most stringent seal $\min_{\rm Alice}\max_{\rm Bob}\bar{F}_{\rm cond}(p, p_{\max})$ is similarly defined.

Since $\bar{F}$ and $\bar{F}_{\rm cond}$ are two different performance indicators, one expects that $\min_{\rm Alice}\max_{\rm Bob}\bar{F}$ and $\min_{\rm Alice}\max_{\rm Bob}\bar{F}_{\rm cond}$ have to be attained by two different sealing schemes and measurement strategies. I show in Sec. III that this is indeed the case for a general N. Nevertheless, for $N \le 5$, optimal sealing scheme and measurement strategies as reflected by the two performance indicators can be chosen to be the same.

III. THE OPTIMAL MEASUREMENT STRATEGY

A. A measurement strategy and its performance

Obviously, $p_{\max}$ is equal to the maximum probability of correctly distinguishing the mixed states ρ_i's with *a priori* occurrence probabilities η_i's. The set of POVM elements $\{\Pi_k\}_{k=0}^{N-1}$ that maximizes such a probability is given by [11, 12]

$$\Pi_k(\eta_k\rho_k - \eta_j\rho_j)\Pi_j = 0 \tag{7}$$

and

$$\sum_i \eta_i\rho_i\Pi_i - \eta_j\rho_j \ge 0 \tag{8}$$

for all $0 \le j, k \le N-1$. In other words, $p_{\max}$ and Π_i's satisfy the equation

$$p_{\max} = \sum_{i=0}^{N-1} \eta_i {\rm Tr}(\Pi_i\rho_i) = \sum_{i=0}^{N-1} \eta_i \langle\tilde{\psi}_i|\Pi_i \otimes I|\tilde{\psi}_i\rangle \ . \tag{9}$$

Clearly, $1/N \le \eta_0 \le p_{\max} \le 1$. In fact, $p_{\max} = 1/N$ if and only if $\rho_i = \rho_j$ for all i, j; and $p_{\max} = 1$ if and only if ρ_i's are mutually orthogonal.

I write the spectral decomposition of Π_i as

$$\Pi_i = \sum_j \mu_{ij}|e_{ij}\rangle\langle e_{ij}| \ , \tag{10}$$

where $\{|e_{ij}\rangle\}_j$ are complete sets of orthonormal state kets for all i and $\mu_{ij} \ge 0$ for all i, j. Based on the Π_i's, I construct

$$M_i = \sum_j \left(\frac{1-\nu}{N} + \nu\mu_{ij}\right)^{1/2} |e_{ij}\rangle\langle e_{ij}| \ , \tag{11}$$

where

$$\nu \equiv \nu(p, p_{\max}, N) = \frac{pN-1}{p_{\max}N-1} \tag{12}$$

for all $p \in [1/N, 1]$. Clearly, $\nu \in [0,1]$ and hence M_i's are well-defined measurement operators. I denote the POVM measurement with Kraus operators $\{M_i\}_{i=0}^{N-1}$ by $\mathcal{E}_{p,p_{\max}}$ for

$$\sum_{i=0}^{N-1} \eta_i \mathrm{Tr}(M_i^\dagger M_i \rho_i) = \frac{1-\nu}{N} + \nu \sum_{i=0}^{N-1} \eta_i \mathrm{Tr}(\Pi_i \rho_i) = p \ . \tag{13}$$

Using the POVM measurement $\mathcal{E}_{p,p_{\max}}$, the probability that Alice's original classical message is i and Bob's measurement on the sealed state yields j is equal to

$$\begin{aligned} \mathrm{Pr}_{ij} &= \eta_i \langle\tilde{\psi}_i|(M_j^\dagger \otimes I)(M_j \otimes I)|\tilde{\psi}_i\rangle \\ &= \eta_i \left[\frac{1-\nu}{N} + \nu \mathrm{Tr}(\Pi_j \rho_i)\right] \ . \end{aligned} \tag{14}$$

In particular, if $p, p_{\max}$ are large and ν is close to 1, then Pr_{ii} is generally much larger than Pr_{ij} for $j \neq i$. Consequently, the mutual information $\mathcal{I}$ is close to the maximum possible value of $-\sum_i \eta_i \log_2 \eta_i$. (For example, in the He's scheme [5], Bob's mutual information obtained by the POVM $\mathcal{E}_{p_{\max},p_{\max}}$ on the sealed message equals $I = 0.99n[1 + \epsilon \log_2 \epsilon + (1-\epsilon)\log_2 \epsilon]$ where ϵ is the small control parameter in his scheme.)

To investigate the disturbance caused by this POVM measurement, I use the following lemma.

Lemma 1. *Let $0 \leq \nu \leq 1$. Then,*

$$\begin{aligned} f(x) &= \sqrt{\nu x + \frac{1-\nu}{N}} - \sqrt{\frac{1-\nu}{N}} \\ &\quad - \left(\sqrt{\nu + \frac{1-\nu}{N}} - \sqrt{\frac{1-\nu}{N}}\right) x \geq 0 \end{aligned} \tag{15}$$

for all $x \in [0,1]$. Besides, the equality holds if and only if $x = 0$ or 1.

Proof. By solving the equation $df/dx = 0$ and considering $d^2 f/dx^2$, I find that the continuous function $f(x)$ has a single local maximum in the interval $[0,1]$. Hence, $f(x) \geq \min(f(0), f(1)) = 0$ for all $x \in [0,1]$. Moreover, $f(x) = 0$ if and only if $x = 0$ or 1. □

A direct consequence of Lemma 1 is that

$$\begin{aligned} M_i &\geq \sqrt{\frac{1-\nu}{N}} I + \left(\sqrt{\nu + \frac{1-\nu}{N}} - \sqrt{\frac{1-\nu}{N}}\right) \Pi_i \\ &\equiv a(\nu, N) I + b(\nu, N) \Pi_i \equiv aI + b\Pi_i \end{aligned} \tag{16}$$

for all i. And the equality holds if and only if Π_i is a projector.

To find a lower bound for $\min_{\mathrm{Alice}} \max_{\mathrm{Bob}} \bar{F}$, I substitute Eq. (16) into Eq. (5) to obtain

$$\begin{aligned} &\min_{\mathrm{Alice}} \max_{\mathrm{Bob}} \bar{F}(p, p_{\max}) \\ &\geq \bar{F}(\mathcal{E}_{p,p_{\max}}) \\ &\geq \sum_{i,j=0}^{N-1} \eta_i \left|\langle\tilde{\psi}_i| aI \otimes I + b\Pi_j \otimes I|\tilde{\psi}_i\rangle\right|^2 \\ &= Na^2 + 2ab + b^2 \sum_{i,j=0}^{N-1} \eta_i \left|\langle\tilde{\psi}_i|\Pi_j \otimes I|\tilde{\psi}_i\rangle\right|^2 \ . \end{aligned} \tag{17}$$

Subjected to the constraints in Eq. (9) and

$$\sum_{j=0}^{N-1} \langle\tilde{\psi}_i|\Pi_j \otimes I|\tilde{\psi}_i\rangle = 1 \tag{18}$$

for all i, the last line of Eq. (17) is minimized if

$$\langle\tilde{\psi}_i|\Pi_j \otimes I|\tilde{\psi}_i\rangle = \begin{cases} p_{\max} & \text{if } i = j \ , \\ \dfrac{1-p_{\max}}{N-1} & \text{if } i \neq j \ . \end{cases} \tag{19}$$

Consequently,

$$\begin{aligned} &\min_{\mathrm{Alice}} \max_{\mathrm{Bob}} \bar{F}(p, p_{\max}) \\ &\geq 1 - \left(\sqrt{\nu + \frac{1-\nu}{N}} - \sqrt{\frac{1-\nu}{N}}\right)^2 \times \\ &\qquad \left[1 - p_{\max}^2 - \frac{(1-p_{\max})^2}{N-1}\right] \end{aligned} \tag{20}$$

for all $1/N \leq p \leq p_{\max}$, where ν is given by Eq. (12).

To find a lower bound for $\min_{\mathrm{Alice}} \max_{\mathrm{Bob}} \bar{F}_{\mathrm{cond}}$, I substitute Eq. (16) into Eq. (6) to obtain

$$\begin{aligned} &\min_{\mathrm{Alice}} \max_{\mathrm{Bob}} \bar{F}_{\mathrm{cond}}(p, p_{\max}) \\ &\geq \bar{F}_{\mathrm{cond}}(\mathcal{E}_{p,p_{\max}}) \\ &\geq \sum_{i=0}^{N-1} \frac{\eta_i \left(a + b\langle\tilde{\psi}_i|\Pi_i \otimes I|\tilde{\psi}_i\rangle\right)^2}{a^2 + \nu\langle\tilde{\psi}_i|\Pi_i \otimes I|\tilde{\psi}_i\rangle} \ . \end{aligned} \tag{21}$$

Note that the function $g(x) = (a+bx)^2/(a^2+\nu x)$ is convex for any $a, b, \nu, x \geq 0$. So by applying Jensen's inequality to the right hand side of Eq. (21) and by using Eq. (9), I conclude that

$$\begin{aligned} \min_{\mathrm{Alice}} \max_{\mathrm{Bob}} \bar{F}_{\mathrm{cond}}(p, p_{\max}) &\geq \frac{(a + bp_{\max})^2}{a^2 + \nu p_{\max}} \\ &= \frac{(a + bp_{\max})^2}{p} \ . \end{aligned} \tag{22}$$

B. The optimality of the measurement strategy with respected to the average fidelity performance measure

For an arbitrary quantum seal chosen by Alice, it may be possible to find a POVM measurement $\mathcal{E}$, whose probability of correctly determining the sealed message equals

p, satisfying $\bar{F}(\mathcal{E}) > \bar{F}(\mathcal{E}_{p,p_{\max}})$. However, Alice may choose the quantum seal reported in the next paragraph. It turns out that the value of $\bar{F}(\mathcal{E})$ for this seal is upper-bounded by the right hand side of Eq. (20). This makes $\mathcal{E}_{p,p_{\max}}$ an optimal measurement strategy for Bob when using $\bar{F}$ as the performance indicator.

Consider the quantum sealing scheme with $\eta_i = 1/N$ and

$$\begin{aligned} |\tilde{\psi}_i\rangle &= p_{\max}^{1/2}|i\rangle_{\rm B}\otimes|i\rangle_{\rm A}\otimes|i\rangle_{\rm A} \\ &\quad + \sqrt{\frac{1-p_{\max}}{N-1}}\sum_{j\neq i}|j\rangle_{\rm B}\otimes|j\rangle_{\rm A}\otimes|i\rangle_{\rm A} \end{aligned} \quad (23)$$

for $i = 0, 1, \ldots, N-1$, where each of the three quantum registers used in the above scheme is N-dimensional with basis $\{|j\rangle\}_{j=0}^{N-1}$. It is straight-forward to check that $|\tilde{\psi}_i\rangle$'s are orthonormal and that

$$\begin{aligned} \rho_i &= {\rm Tr}_{\rm A}(|\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|) = p_{\max}|i\rangle\langle i| + \frac{1-p_{\max}}{N-1}(I - |i\rangle\langle i|) \\ &= \frac{(p_{\max}N-1)|i\rangle\langle i| + (1-p_{\max})I}{N-1} \\ &\equiv c(p_{\max},N)|i\rangle\langle i| + d(p_{\max},N)I \\ &\equiv c|i\rangle\langle i| + dI \ . \end{aligned} \quad (24)$$

Now I show that this sealing scheme is the most stringent one in the sense that the resultant fidelity of the quantum state after any POVM measurement by Bob is upper-bounded by the right hand side of Eq. (20). Recall that $\mathcal{E}$ can be written as $\sum_{i=0}^{N-1}\mathcal{L}_i$ where $\mathcal{L}_i$ is the super-operator describing Bob's action when he concludes that the sealed message is i. In general, the action of each $\mathcal{L}_i$ on a density matrix ρ can be written as

$$\mathcal{L}_i(\rho) = \sum_j Q_{ij}\rho Q_{ij}^\dagger \ . \quad (25)$$

Clearly, Q_{ij}'s satisfy

$$\sum_{i,j} Q_{ij}^\dagger Q_{ij} = I \quad (26)$$

and

$$\frac{1}{N}\sum_{i,j}{\rm Tr}(Q_{ij}^\dagger Q_{ij}\rho_i) = p \ . \quad (27)$$

From Eqs. (5) and (23), the average fidelity of the state after Bob has applied the POVM $\mathcal{E}$ is given by

$$\begin{aligned} \bar{F} &= \frac{1}{N}\sum_{i,j,k}|c\langle i|Q_{jk}|i\rangle + d{\rm Tr}(Q_{jk})|^2 \\ &= \frac{c^2}{N}\sum_{i,j,k}|\langle i|Q_{jk}|i\rangle|^2 + d(d+\frac{2c}{N})\sum_{j,k}|{\rm Tr}(Q_{jk})|^2 \\ &\leq \frac{c^2}{N}\sum_{i,j,k,m}\langle i|Q_{jk}^\dagger|m\rangle\langle m|Q_{jk}|i\rangle \\ &\qquad + d(d+\frac{2c}{N})\sum_{j,k}|{\rm Tr}(Q_{jk})|^2 \\ &= c^2 + d(d+\frac{2c}{N})\sum_{j,k}|{\rm Tr}(Q_{jk})|^2 \ , \end{aligned} \quad (28)$$

where the equality holds if and only if $\langle i|Q_{jk}|m\rangle = 0$ for all $i \neq m$. Subjected to the constraints in Eqs. (26) and (27), the last line of Eq. (28) is maximized if

$$\begin{aligned} Q_{i0} &= \sqrt{\frac{p_{\max}-p+Np-1}{p_{\max}N-1}}|i\rangle\langle i| \\ &\quad + \sqrt{\frac{p_{\max}-p}{p_{\max}N-1}}\sum_{j\neq i}|j\rangle\langle j| \\ &= a(\nu,N)I + b(\nu,N)|i\rangle\langle i| \ , \end{aligned} \quad (29)$$

and $Q_{ij} = 0$ for all $j \neq 0$. (Note that although this set of Q_{ij}'s is not unique, it is straight-forward to check that all Q_{ij}'s that maximizes $\bar{F}$ are equivalent in the sense that they give the same POVM $\mathcal{E}$.) In addition, the maximum probability $p_{\max}$ of distinguishing ρ_i's is attained by the measurement operators $|i\rangle\langle i|$'s as these operators satisfy Eqs. (7) and (8). Therefore, $Q_{i0} = M_i$ for all i and hence $\mathcal{E} = \mathcal{E}_{p,p_{\max}}$. Consequently, for this particular quantum seal chosen by Alice, $\bar{F}$ is at most equal to the right hand side of Eq. (20). Besides, such an equality can be obtained by using the POVM $\mathcal{E}_{p,p_{\max}}$. That is to say, $\mathcal{E}_{p,p_{\max}}$ is an optimal measurement strategy for Bob with respected to the average fidelity performance measure when Alice uses the sealing scheme in Eq. (23).

C. Analysis of the measurement strategy with respected to the average conditional fidelity performance measure

Using the same notation as in Subsec. III B, the average conditional fidelity of the state after Bob has applied the POVM $\mathcal{E}$ to the quantum seal in Eq. (23) equals

$$\bar{F}_{\rm cond} = \frac{1}{N}\sum_{i=0}^{N-1}\frac{\sum_j|c\langle i|Q_{ij}|i\rangle + d{\rm Tr}(Q_{ij})|^2}{\sum_j\left[c\langle i|Q_{ij}^\dagger Q_{ij}|i\rangle + d{\rm Tr}(Q_{ij}^\dagger Q_{ij})\right]} \ . \quad (30)$$

By constrained extremization, it is easy to show that for a fixed value of $\sum_j\left[c\langle i|Q_{ij}^\dagger Q_{ij}|i\rangle + d{\rm Tr}(Q_{ij}^\dagger Q_{ij})\right]$, the

ith term in the above equation is maximized if (1) $Q_{ij}=0$ for all $j\neq 0$, (2) $|k\rangle$ is an eigenvector of Q_{i0} whose eigenvalue $\tau_{ik}\geq 0$ for all k, (3) $\tau_{ik}=\tau_{ik'}$ for all $k,k'\neq i$, and (4) $\tau_{ii}\geq\tau_{ik}$ for all $k\neq i$. However, one cannot jump to the conclusion that $\bar{F}_{\rm cond}$ is maximized by picking $Q_{i0}=a(\nu,N)I+b(\nu,N)|i\rangle\langle i|$. Actually, this conclusion is wrong in general. A counterexample is given below: let $N=8$, $p_{\rm max}=0.9$ and $p=0.3$. By choosing $Q_{i0}=a(\nu,N)I+b(\nu,N)|i\rangle\langle i|$, $\bar{F}_{\rm cond}=0.980204$. In contrast, by choosing $Q_{i0}=3(2\sqrt{47}|i\rangle\langle i|+\sqrt{13}\sum_{j\neq i}|j\rangle\langle j|)/15\sqrt{31}$ for $i=0,1,\ldots,5$ and $Q_{i0}=(2\sqrt{109}|i\rangle\langle i|+3\sqrt{29}\sum_{j\neq i}|j\rangle\langle j|)/5\sqrt{31}$ for $i=6,7$, then $\bar{F}_{\rm cond}=0.981247$. That is to say, for $p_{\rm max}=0.9$ and $p=0.3$, the $\bar{F}_{\rm cond}$ caused by a certain asymmetric set of Kraus operators $\{Q_{i0}\}$ (in the sense that there exist i,j such that $Q_{i0}\neq UQ_{j0}U^{-1}$ for some permutation operation U of the standard basis) is greater than that caused by a symmetric set of Kraus operators. In fact, this symmetry breaking phenomenon is partly due to the fact that $\bar{F}_{\rm cond}(\mathcal{E})$, unlike $\bar{F}(\mathcal{E})$, is not a linear function of $\mathcal{E}$. And the nonlinear dependence of $\bar{F}_{\rm cond}$ on $\mathcal{E}$ makes the determination of $\min_{\rm Alice}\max_{\rm Bob}\bar{F}_{\rm cond}(p,p_{\rm max})$ difficult.

In spite of this difficulty, the function $\min_{\rm Alice}\max_{\rm Bob}\bar{F}_{\rm cond}(p,p_{\rm max})$ can be found in the following three special cases: (1) $N\leq 5$, (2) $p=1/N$ and (3) $p=p_{\rm max}$.

For the first case ($N\leq 5$), by constrained maximization, the ith term in Eq. (30) is upper-bounded by $h(x_i)=[a(\nu(x_i,p_{\rm max},N),N)+b(\nu(x_i,p_{\rm max},N),N)p_{\rm max}]^2/x_i$, where $x_i=\sum_j\left[c\langle i|Q_{ij}^\dagger Q_{ij}|i\rangle+d{\rm Tr}(Q_{ij}^\dagger Q_{ij})\right]/\sum_j{\rm Tr}(Q_{ij}^\dagger Q_{ij})$. Observe that $h(x)$ is concave for $N\leq 5$ and $p\in[1/N,p_{\rm max}]$. (One way to see this is to use Mathematica to check that $h''(p)\leq 0$.) Therefore, Eq. (30) is upper bounded by $h(p)=(a+bp_{\rm max})^2/p$ if $N\leq 5$. Surely, this upper bound is attained by picking the POVM $\mathcal{E}_{p,p_{\rm max}}$, namely, the one that also maximizes the performance indicator $\bar{F}$.

The second case ($p=1/N$) is trivial as Eq. (22) implies that the average conditional fidelity of the state after applying $\mathcal{E}_{1/N,p_{\rm max}}$ equals 1.

For the third case ($p=p_{\rm max}$), the symmetry of the quantum seal in Eq. (23) demands that the denominator in each term of the sum in Eq. (30) must all equal to $p_{\rm max}$. Using the same constrained maximization analysis in the first case, each term in Eq. (30) is upper-bounded by $h(p_{\rm max})=p_{\rm max}$. Hence, $\bar{F}_{\rm cond}\leq p_{\rm max}$ in this case. Moreover, this upper bound is attained by the POVM $\mathcal{E}_{p_{\rm max},p_{\rm max}}$.

In summary, I have proven

Theorem 1. *Let $1/N\leq p\leq p_{max}$. Then,*

$$\min_{Alice}\max_{Bob}\bar{F}(p,p_{max})=1-\left(\sqrt{\nu+\frac{1-\nu}{N}}-\sqrt{\frac{1-\nu}{N}}\right)^2\left[1-p_{max}^2-\frac{(1-p_{max})^2}{N-1}\right] \tag{31}$$

and

$$\min_{Alice}\max_{Bob}\bar{F}_{cond}(p,p_{max})\geq\frac{\left[\sqrt{\frac{1-\nu}{N}}+\left(\sqrt{\nu+\frac{1-\nu}{N}}-\sqrt{\frac{1-\nu}{N}}\right)p_{max}\right]^2}{p}\ , \tag{32}$$

where ν is given by Eq. (12). In particular, Eq. (32) is an equality if $p=1/N, p_{max}$ or $N\leq 5$. Furthermore,

$$\min_{Alice}\max_{Bob}\bar{F}(p_{max},p_{max})=p_{max}^2+\frac{(1-p_{max}^2)}{N-1} \tag{33}$$

and

$$\min_{Alice}\max_{Bob}\bar{F}_{cond}(p_{max},p_{max})=p_{max}\ . \tag{34}$$

Figs. 1 and 2 show $\min_{\rm Alice}\max_{\rm Bob}\bar{F}(p,p_{\rm max})$ and $\min_{\rm Alice}\max_{\rm Bob}\bar{F}_{\rm cond}(p,p_{\rm max})$ *vs.* p for different $p_{\rm max}$ when $N=2,4$. Note that $\min_{\rm Alice}\max_{\rm Bob}\bar{F}(p,p_{\rm max})$ and $\min_{\rm Alice}\max_{\rm Bob}\bar{F}_{\rm cond}(p,p_{\rm max})$ are discontinuous at $p=1/N$ whenever $p_{\rm max}>1/N$. This discontinuity originates from the sudden change in the dimension of the set $\{\rho_i\}_{i=0}^{N-1}$ around the point $p=1/N$ [8]. Besides, $\min_{\rm Alice}\max_{\rm Bob}\bar{F}(p,p_{\rm max})\to 1-p(1-p_{\rm max}^2)/p_{\rm max}$. Note also that $\min_{\rm Alice}\max_{\rm Bob}\bar{F}(p,p_{\rm max})$ is a concave function of p for a fixed value of $p_{\rm max}$ for $\bar{F}(\mathcal{E})$ is a linear function of $\mathcal{E}$.

Finally, I remark that derivations of the upper and lower bounds for $\min_{\rm Alice}\max_{\rm Bob}\bar{F}(p,p_{\rm max})$ and $\min_{\rm Alice}\max_{\rm Bob}\bar{F}_{\rm cond}(p,p_{\rm max})$ reported in this Section

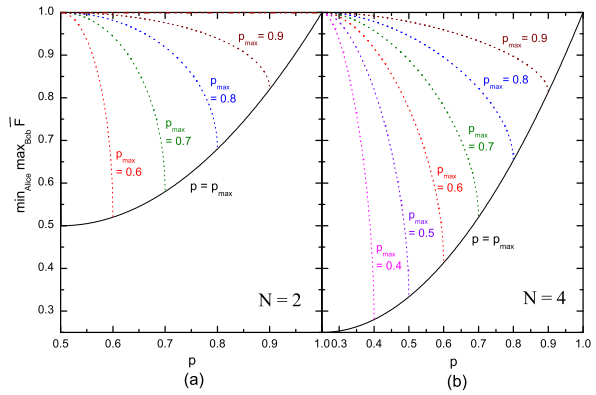

FIG. 1: (Color online) Dotted curves show $\min_{\rm Alice}\max_{\rm Bob}\bar{F}(p,p_{\max})$ *vs.* p for various values of $p_{\max}$ with (a) $N=2$ and (b) $N=4$. The solid curves show the case of $p=p_{\max}$.

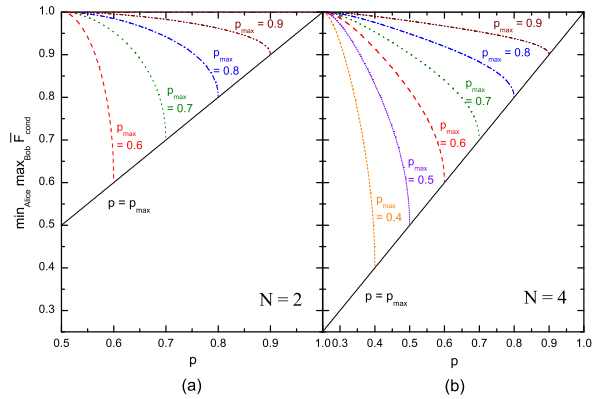

FIG. 2: (Color online) Dotted curves show $\min_{\rm Alice}\max_{\rm Bob}\bar{F}_{\rm cond}(p,p_{\max})$ *vs.* p for various values of $p_{\max}$ with (a) $N=2$ and (b) $N=4$. The solid curves show the case of $p=p_{\max}$.

are also valid in the case of determining partial information on the original message via the partition $\mathfrak{P}$.

IV. PROOF OF INSECURITY OF QUANTUM SEAL

Although the functional form of $\min_{\rm Alice}\max_{\rm Bob}\bar{F}_{\rm cond}(p,p_{\max})$ is not known for $N>5$ and $1/N<p<p_{\max}$, its lower bound stated in Theorem 1 is already sufficiently stringent to help proving the insecurity of quantum seal. Specifically, to fix $\nu=1/2$ by choosing the appropriate p, Theorem 1 implies the existence of a POVM measurement $\mathcal{E}_{p,p_{\max}}$ that make both $\min_{\rm Alice}\max_{\rm Bob}\bar{F}$ and $\min_{\rm Alice}\max_{\rm Bob}\bar{F}_{\rm cond}$ greater than $1/2$ for all $N\geq 2$. In other words, this measurement obtains non-trivial information on the sealed message and escapes verifier's detection at least half of the time. Hence, all quantum seals are insecure.

In fact, the major loophole in He's proof of the security of his quantum string seal in Ref. [5] is that he incorrectly assumed that measuring all the qubits is the only method to obtain a significant portion of information of the sealed message.

Recently, He proposed the following method of attack [13]: Bob measures the sealed message using Π_i's as the POVM elements with probability $1/2$; and he randomly guesses the sealed message without actually measuring otherwise. His mixed strategy escapes verifier's detection at least half of the time (as measured by $\bar{F}$) and obtains non-trivial information on the sealed message. Nevertheless, $\bar{F}_{\rm cond}$ of this strategy approaches $p_{\max}/2$ as $N\to\infty$. Compared with Theorem 1, the average conditional fidelity of He's attack is only about $1/2$ that of the optimal strategy.

V. CONCLUSIONS

To summarize, I have extended the study of information disturbance tradeoff for quantum bit seal [8] to the case of quantum string seal. Specifically, I show that the average fidelity and average conditional fidelity of the measured state is greater than or equal to the right hand side of Eqs. (31) and (32), respectively. Furthermore, the equalities are simultaneously attained by a specific quantum sealing scheme provided that $N\leq 5$ or $p=1/N, p_{\max}$. A consequence of this information disturbance tradeoff expression is that all quantum seals are insecure provided that one has access to a quantum computer.

One of the major reasons I can extend the earlier result on quantum bit seal in Ref. [8] here is that I replace the classical L_1 distance by the probability of distinguishing two classical probability distributions. The later concept readily extends to the case of $N>2$. Actually, it can be shown that for $N=2$ the measurement $\mathcal{E}_{p,p_{\max}}$ together with the expression for $\min_{\rm Alice}\max_{\rm Bob}\bar{F}(p,p_{\max})$ are the same as the ones reported in Ref. [8]. I also remark that even though I consider only the case of sealing finite number of messages, the arguments used in this Paper can be easily extended to cover the case of sealing infinite number of messages using states in an infinite dimensional Hilbert space.

Although quantum seal is not unconditionally secure, the construction of $\mathcal{E}_{p,p_{\max}}$ requires Bob to find the POVM measurement $\{\Pi_i\}$ that distinguish the density matrices ρ_i's with *a priori* probability η_i's with minimum error. In general, it is difficult to explicitly find the Π_i's; and a quantum computer is needed to implement $\mathcal{E}_{p,p_{\max}}$. So, it may be possible to construct a quantum seal that is secure under certain computational or hardware assumptions. Last but not least, it is instructive to find $\min_{\rm Alice}\max_{\rm Bob}\bar{F}_{\rm cond}$ for $N>5$ and $1/N<p<p_{\max}$.

Acknowledgments

Useful discussions with K. H. Ho is gratefully acknowledged. This work is supported by the RGC grant HKU 7010/04P of the HKSAR Government.

[1] H. Bechmann-Pasquinucci, Int. J. Quant. Inform. **1**, 217 (2003).
[2] H. F. Chau, *Sealing quantum message by quantum code*, quant-ph/0308146.
[3] S. K. Singh and R. Srikanth, Physica Scripta **71**, 433 (2005).
[4] G.-P. He, *Quantum secret sharing, hiding and sealing of classical data against collective measurement*, quant-ph/0502091v1.
[5] G.-P. He, Int. J. Quant. Inform. **4**, 677 (2006).
[6] H. Bechmann-Pasquinucci, G. M. D'Ariano, and C. Macchiavello, Int. J. Quant. Inform. **3**, 435 (2005).
[7] G.-P. He, Phys. Rev. A **71**, 054304 (2005).
[8] H. F. Chau, Phys. Lett. A **354**, 31 (2006).
[9] H. Buhrman, M. Christandl, P. Hayden, H.-K. Lo, and S. Wehner, *On the (im)possibility of quantum string commitment*, quant-ph/0504078.
[10] H. Buhrman, M. Christandl, P. Hayden, H.-K. Lo, and S. Wehner, *Security of quantum bit string commitment depends on the information measure*, quant-ph/0609237, to appear in Phys. Rev. Lett.
[11] A. S. Holevo, J. Multivar. Anal. **3**, 337 (1973).
[12] H. P. Yuen, R. S. Kennedy, and M. Lax, IEEE Trans. Inform. Theo. **21**, 125 (1975).
[13] G.-P. He, *Secure quantum string seal exists*, quant-ph/0602159.